# Protokoll
# der 8. Sitzung der GMDS-Arbeitsgruppe
# *Datenschutz in Krankenhausinformationssystemen*
# am 12./13. Mai 1997 in Magdeburg

Die Sitzung fand im Institut für Biometrie und Medizinische Informatik der Otto-von-Guericke-Universität statt.

**Sitzungszeit:** Montag, 12.5.1997, 14.30 bis 18.30 Uhr,
Dienstag, 13.5.1997, 9.00 bis 12.00 Uhr.

**Anwesend:**
Dr. B. Blobel (Magdeburg)
Dr. R. Killmann (Erlangen)
R. Krohn (Magdeburg)
P. Pharow (Magdeburg)
M. Pöll (Innsbruck)
Prof. Dr. K. Pommerening (Mainz)
M. Schnabel (München)
V. Spiegel (Magdeburg)
J. Walther (Krefeld)
S. Wolf (Kiel)

**Entschuldigt:**
Dr. T. Berger (Krefeld)
G. Bleumer (Florham Park)
Dr. B. Hornung (Marburg)
Dr. M. Hortmann (Bremen)
H. Leitgeb (Salzburg)
Dr. J. Paczkowski (Troisdorf)
Dr. H. Ruelius (Göttingen)
Prof. Dr. K. Sauter (Kiel)
Dr. K.-H. Schicketanz (Mainz)
M. Schurer (Tübingen)
W. Thoben (Oldenburg)

**Tagesordnung:**
1. Festlegung der Tagesordnung
2. Protokoll der vorigen Sitzung
3. Mitteilungen und Berichte
4. ZVEI-Arbeitskreis »Vernetzung und Archivierung«
5. Outsourcing von Archivleistungen und Datenschutz
6. EU- und Chipkartenprojekte
7. Leitlinien zum Datenschutz
8. Musterkonzept
9. Weiteres Vorgehen der Arbeitsgruppe
10. Verschiedenes

Der Vorsitzende begrüßt die Teilnehmer und dankt Herrn Blobel und seinen Mitarbeitern für die Organisation der Sitzung. Da neue Teilnehmer anwesend sind, stellen sich die Teilnehmer kurz vor.

**TOP 1. Festlegung der Tagesordnung**

Die mit der Einladung verschickte Tagesordnung wird um die oben genannten Punkte 4 und 8 ergänzt und in dieser Form angenommen.

**TOP 2. Protokoll der vorigen Sitzung**

Das Protokoll der 7. Sitzung der Arbeitsgruppe wird in TOP 11 korrigiert zu: »Das nächste Treffen soll am 12. und 13. Mai 1997 in Magdeburg stattfinden.« Es wird in der korrigierten Form angenommen.

**TOP 3. Mitteilungen und Berichte**

a) Der Beitrag der AG für den GMDS-Jahresbericht 1997 liegt vor und ist im Internet zugänglich; er gilt für die Periode 1. Juli 1996 bis 30. Juni 1997. Hauptereignisse waren in diesem Zeitraum:

- die Erstellung der Anleitung für das Management,
- die Mitorganisation der KIS97.

b) Herr Pommerening weist auf einige neue Internet-Ressourcen hin, die auch über die WWW-Seite der AG erreichbar sind:

- CERT-Empfehlungen zur sicheren Systemkonfiguration, z. B.
    - Security tools.
    - UNIX configuration guidelines.
- Sicherheitskriterien (ITSEC, Common Criteria, Rainbow series).
- Die Landesdatenschutzbeauftragten von
    - Bayern,
    - Berlin,
    - Brandenburg,
    - Hamburg,
    - Rheinland-Pfalz,
    - Saarland,
    - Schleswig-Holstein

  und ihre neuesten Tätigkeitsberichte.

- Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen (Entschließung der 53. Konferenz der Datenschutz-beauftragten des Bundes und der Länder vom 17./18. April 1997)
- OECD: Security, privacy, cryptography and intellectual property rights mit Link auf »Guidelines on the Protection of Privacy and Transborder Flows of Personal Data«
- Der SAVE-AK Datenschutz.
- Guidelines von Ross Anderson (Clinical System Security)
- Das TC TrustCenter, an dessen Aufbau Herr Hortmann beteiligt ist und das von der belgischen Ärztekammer genutzt werden wird.

- Das MedSec-Projekt des DFN.
- Die Zeitschrift »Datenschutz und Datensicherheit«.
- Die DFN-Mitteilungen.
- Die DFG (Deutsche Forschungsgemeinschaft).

c) Herr Pommerening berichtet über neue Erkenntnisse zur Sicherheit von Standardsoftware. Besondere Risiken stellen im Bereich des World Wide Web der Microsoft-Internet-Explorer sowie ActiveX-Applets dar, deren Verwendung dazu führen kann, dass ein einziger argloser Benutzer die Sicherheit eines Firewall-Systems beseitigt. Fazit: »Aktive« Dokumente sind ein grundsätzliches Sicherheitsrisiko; das galt schon lange für ASCII-Texte, wenn der ANSI-Treiber installiert ist, und für Postscript-Dokumente mit eingebauten Systembefehlen. Aktuell ist das Problem bei MS-Word und anderer Software mit eingebauten Makro-Fähigkeiten und im WWW bei HTML mit Applets. Solche Möglichkeiten werden nach seiner Einschätzung nie sicher nutzbar sein. Weiterhin ist in letzter Zeit bekannt geworden, daß Passwörter unter Windows-NT im Klartext im Speicher gehalten werden und von dort leicht über das Netz für jedermann auslesbar sind. Neue Informationsquellen im Internet sind

- NetWare Hack FAQ,
- Web Hack FAQ.

Die Firmen AccessData und Crak Software bieten Passwort-Rekonstruktionsdienste für Standard-Software im Internet an.

d) Herr Pommerening berichtet, dass das Signaturgesetz im Bundesrat gescheitert ist; aus dem Innenministerium gibt es Pläne zur obligatorischen Schlüsselhinterlegung. Der BVMI ist an die AG herangetreten mit der Bitte um Formulierungshilfe für eine eventuelle Resolution. Nach Ansicht der AG ist wirksamer Datenschutz mit einer Vorschrift zur Hinterlegung kryptographischer Schlüssel nicht möglich. Da das Thema aber zurzeit in der Öffentlichkeit ausführlich diskutiert wird und alle wesentlichen Argumente bekannt sind, wäre eine weitere Resolution höchstens dann noch effektiv, wenn Sie von einer ärztlichen Standesvereinigung käme.

e) Herr Pommerening berichtet von der Fachtagung KIS97, auf der Datenschutz ein Schwerpunktthema war. Es gab Vorträge von I. Geis, B. Blobel und R. Wellbrock/R. Wehrmann vom Hessischen Datenschutzbeauftragten sowie einen Workshop mit Vorträgen von M. Schnabel und H. Bachleitner. Die Diskussion zeigte, dass in der Praxis noch erheblicher Aufklärungsbedarf und große Sicherheitslücken bestehen und dass der Bedarf an konkreten Hilfestellungen groß ist. Als Themenvorschläge für die nächste KIS-Tagung werden von der AG genannt: der elektronische Berufsausweis (Health Professional Card) und die Sicherheit in verteilten Architekturen. Die nächste Sitzung der KIS-AG wird am 13.6.1997 in Marburg stattfinden.

f) Neue Veröffentlichungen aus der AG:

- G. Bleumer, M. Schunter: Datenschutzorientierte Abrechnung medizinischer Leistungen, DuD Heft 2/97.
- B. Blobel, K. Pommerening: Datenschutz und Datensicherheit in Informationssystemen des Gesundheitswesens. Führen & Wirtschaften im Krankenhaus 2/1997, 133-138.
- B. Blobel, K. Pommerening: Datenschutz und Datensicherheit in öffentlichen Netzen im Gesundheitswesen. Forum der Medizin-Informatik 1 (1997), 10-13.

- B. Blobel: Datenschutz in Gesundheitsinformationssystemen. Krankenhausumschau 12 (1996).
- B. Blobel: Bedrohungen und Lösungen für Datenschutz und Datensicherheit in Informationssystemen des Gesundheitswesens. In: K. Kuhn u. a. (Hrsg.): Praxis der Informationsverarbeitung im Krankenhaus. ecomed, Landsberg 1997, 1 - 18.
- M. Schnabel: Datenschutz in der Krankenhauspraxis. In: K. Kuhn u. a. (Hrsg.): Praxis der Informationsverarbeitung im Krankenhaus. ecomed, Landsberg 1997, 97 - 106.

**TOP 4. ZVEI-Arbeitskreis »Vernetzung und Archivierung«**

Herr Killmann stellt den Entwurf eines Positionspapiers zu Datenschutz und Telemedizin dieses Arbeitskreises vor. Es ist gedacht als »Beitrag zur Schaffung sinnvoller Regelungen auf nationaler und internationaler Ebene zu dem Thema Telemedizin und insbesondere dem sensiblen Bereich des Datenschutzes bei Übertragung und Archivierung medizinischer Bilddaten«.

Die AG begrüßt die Aktivität zur Verbesserung des Datenschutzes. Die AG ist allerdings der Meinung, dass in einem solchen Positionspapier nach dem Stand der Technik mögliche Maßnahmen nicht zugunsten von Kompromissen mit der gegenwärtigen Praxis unberücksichtigt bleiben sollten. In der Detail-Diskussion werden folgende Punkte genannt:

- Die Authentisierung durch Passwörter wird als zu schwach angesehen; es sollte der Einsatz einer elektronischen Ausweiskarte verlangt werden.
- Die Verschlüsselung bei der Datenspeicherung sollte auch im »geschützten« Bereich eines Krankenhauses gefordert werden, da sie die Sichtbarkeit sensibler Daten auch für das IT-Personal einschränkt und eine bessere Zugriffskontrolle ermöglicht.

**TOP 5. Outsourcing von Archivleistungen und Datenschutz**

Herr Walther stellt das geplante Telearchiv-Servicecenter von Mediagate vor, das am 1.8.1997 den Pilotbetrieb aufnehmen soll. Die Daten werden dort verschlüsselt abgegeben (»Garderoben-Prinzip«) und sind für Mitarbeiter des Dienstleistungsunternehmens nicht lesbar. Herr Pommerening weist in diesem Zusammenhang noch einmal auf die Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 hin; insbesondere wird dort für das Outsourcing gefordert, dass die Daten wegen des Erhaltes der Beschlagnahmefestigkeit im Krankenhaus lokalisiert bleiben sollten. Der kryptografische Schutz der archivierten Daten könnte diese Bedenken gegenstandslos machen; als problematisch hierfür sieht die AG allerdings an, dass die Schlüsselverwaltung dem BSI, also einer Bundesbehörde, übertragen werden soll. Geklärt werden sollte außerdem die Frage, wie weit durch ein Leasing-Verfahren für Archiv-Datenträger der ärztliche Gewahrsam für die Daten beibehalten werden kann.

**TOP 6. EU- und Chipkartenprojekte**

Herr Blobel berichtet über die Projekte

1. HANSA (Healthcare Advanced Network System Architecture),
2. ISHTAR (Implementing Secure Healthcare Telematics Applications in Europe),
3. TrustHealth 1 (Trustworthy Health Telematics),
4. DIABCARD 3 (Improved Communication in Diabetes Care Based on Chipcard Technology),

5. EUROMED-ETS (Trusted Third Party Services for Health Care in Europe),
6. MEDSEC (Health Care Security and Privacy in the Information Society),

an denen die Universität Magdeburg beteiligt ist. Die Bundesärztekammer plant die Einführung des elektronischen Arztausweises (Health Professional Card) bis 1999.

Herr Krohn stellt das ISHTAR-Projekt detaillierter vor. Magdeburg ist ein Verifikations-Center. Es wird die Implementierung einer Security Policy mit dem Werkzeug SIDERO getestet. Ziel ist die Verbesserung der SEISMED-Guidelines, die z. B. im Bereich der Netz-Sicherheit noch recht mangelhaft sind.

Herr Pharow berichtet über TrustHealth. In Magdeburg werden TTP-Dienste zunächst als Pilotprojekt in kleinem Rahmen aufgebaut. Die Ausweiskarten enthalten drei verschiedene private Schlüssel: je einen für Verschlüsselung, elektronische Unterschrift und Authentisierung. Als Leser werden multifunktionale Kartenterminals nach dem MKT-Standard eingesetzt.

Im Anschluss stellt Herr Blobel noch das CORBA-Sicherheitskonzept im Überblick und mit einigen Details vor. Er weist darauf hin, dass der mit CORBA konkurrierende, von Microsoft entwickelte Standard OLE nicht sauber objektorientiert ist und keine Sicherheitsmechanismen vorsieht.

**TOP 7. Leitlinien zum Datenschutz**

Herr Pommerening fasst den aktuellen Stand zusammen: Zu den Aufgaben der Arbeitsgruppe gehört die Ausarbeitung konkreter Leitlinien und Handlungsanweisungen in geeigneter Form. Hierzu wurde bisher schon einiges erarbeitet; insgesamt ist die Sammlung aber teilweise noch unsystematisch und konkretisierungsbedürftig. Wegen der Komplexität des Themas kann auch keine erschöpfende Vollständigkeit angestrebt werden. Als leitlinienartiges Grundsatzpapier für das Krankenhaus-Management ist die Arbeit gedacht, die in f&w erschienen ist und mit diesem Protokoll versendet wird. Leitlinien-Funktion hat auch die Sammlung von Stellungnahmen der Landesdatenschutzbeauftragten, die nach Themen geordnet über den WWW-Server der Arbeitsgruppe zugänglich ist. Ferner gibt es die Empfehlungen zum Internet-Anschluß und zum Umgang mit Standard-Software, die auf der KIS97-Tagung verteilt wurden, die aber nur schwer aktuell zu halten sind.

Material für Leitlinien bieten auch die SEISMED-Guidelines, die bisher von der Arbeitsgruppe nicht ausgewertet werden konnten und viel zu umfangreich und zu wenig praktikabel erscheinen, sowie die Checklisten aus dem Buch »Datenschutz und Datensicherheit« von Herrn Pommerening, die aber aktualisiert und speziell für Einrichtungen des Gesundheitswesens angepasst werden müssten. Für Einzelfragen geeignet scheint auch eine FAQ-Liste, für die Herr Pommerening einen allerersten Entwurf vorlegt. Die AG ist sich darüber einig, dass konkrete Leitlinien, differenziert nach Zielgruppen, vordringlich erarbeitet werden sollen; Vorschläge sollen rechtzeitig vor der nächsten Sitzung vorgelegt werden.

**TOP 8. Musterkonzept**

Die Arbeit an einem zusammenfassenden umfangreichen Musterkonzept, die vor zwei Jahren schon begonnen worden war, soll ebenfalls fortgeführt werden. Herr Blobel schlägt dafür Buchform vor und will noch in diesem Jahr einen weiter ausgebauten Entwurf erstellen. Herr Pommerening berichtet von der zurzeit in Mainz anstehenden Neufassung des DV-Konzepts

der Universitätsklinik, das auch ausführlich zu Datenschutz und -sicherheit Stellung nehmen soll. Herr Blobel beschreibt die in Magdeburg geplanten Änderungen in der Verwaltung der Zugriffsrechte, die sich nach Einführung der elektronischen Ausweiskarte ergeben werden.

**TOP 9. Weiteres Vorgehen der Arbeitsgruppe**

Das weitere Vorgehen wurde bereits in den Tagesordnungspunkten 7 und 8 besprochen.

**TOP 10. Verschiedenes**

a) Der Vorschlag, die AG in »Arbeitsgruppe Datenschutz in Gesundheitsinformationssystemen« umzubenennen, wird einhellig gebilligt. Herr Pommerening will das Prozedere hierzu klären.

b) Das nächste Treffen soll am 11. und 12. Dezember 1997 in Mainz stattfinden.

---

Protokoll: Prof. Dr. K. Pommerening, 13.7.1997, letzte Änderung: 13.7.1997
E-Mail: Pommerening@imsd.uni-mainz.de